ソルパック
Acronis Cyber Protect Cloud Advanced Security + EDR でセキュリティ体制を強化

Acronis Cyber Protect Cloud Advanced Security + EDR は効率的な運用でアラート疲労を軽減。セキュリティとバックアップの融合で、運用負担のない事業継続計画を実現しています。

事業の概要

株式会社ソルパック（以下、ソルパック）は「ITを中心により良い社会づくりに貢献すること」を理念に、1997年に創業されたITサービス企業です。日本IBM製品の販売・サポートから事業をスタートしてビジネスを拡大。現在は7事業部でさまざまなソフトウェアの導入支援やシステムの設計開発、稼働後の保守運用、パソコンのキッティング、BPO（ビジネス・プロセス・アウトソーシング）、IT技術者向けの研修プログラムなどを提供しています。主に中堅中小企業向けに「低価格・高品質・短納期で最適なソリューション」を提供すべくビジネスを展開していますが、時には欧州SAPのERP（統合基幹業務システム）導入など大企業向けの案件も手掛けます。従業員数400人超で、本社のほか国内にテクニカルセンターや開発センターを有しています。

ビジネス上の課題

従来はエンドポイント保護としてウイルスチェックの目的でオンプレミスのソフトを使っていましたが、コロナ禍を契機にリモートワークが増え、従業員が社外に持ち出す業務用PCのセキュリティ対策の強化が課題に挙がっていました。

「システムの保守運用などで現場に出ている一部の社員向けにはVPN環境を提供していましたが、全社員に同じ環境を提供するのはコスト的に困難。しかし従来のセキュリティソフトでは、社外にあるPCを管理下に置くことができず、運用面で不安が残っていました。クラウドサービスを利用したリモートワークが常態化していくなかで、新たなセキュリティ基盤を構築する必要がありました」（管理本部の下田絵理本部長）

こうしたなかで2023年初頭、一部のPCやサーバーがマルウェアに感染するインシデントが発生。管理本部の松島雅秀情報システムマネージャーは「幸いにも被害は一部で業務への影響は最小限にとどまりましたが、同じ事態を繰り返さないための対応は急務でした」と振り返ります。

課題の一つはマルウェアの侵入を検知できなかったことです。「サイバー攻撃は高度化しており、既存のアンチウイルスソフトのみでは不十分だと痛感しました。クラウド環境を含めてネットワーク上の端末の挙動を監視していち早く脅威を見つけ出すEDR（Endpoint Detection and Response）の導入は必然でした」（下田本部長）

業種・業態
ITサービス業

主な課題
- 脅威の迅速な検知
- 有事のPCの速やかな復元
- 使用が簡単な操作環境の実現

主な要件
- クラウド型EDRであること
- 簡単に使用できること
- 日本語サポートがあること

保護対象リソース
- リモートワークなどに使用する業務用PC

主なメリット
- 特別な教育なしで全社展開できる
- 脅威の検知への対処が容易
- PC端末の復元が可能

SOLPAC

Copyright © 2003-2024 Acronis International GmbH.

実際にマルウェア感染を経験したことで、ファイルサーバーはもとより、従業員が利用しているPCのバックアップを取る重要性にも気付かされたと言います。ソルパックでは業務に必要なデータは基本的にファイルサーバーで管理し、バックアップは、サーバーで扱うデータのみを対象としていました。PCには作業中のファイルなどわずかなデータしか残しませんが、それでも「作業中のデータを失い、そのうえでPCをリストアしてゼロから復元していくと業務効率は大きく低下します。インシデントに備えるためにはサーバーはもちろん、PCもバックアップを取っておく必要があると実感しました。またサーバーのデータは常時バックアップを取っていましたが、バックアップしたデータがウイルスに感染していないかを簡単に確認できないこともネックでした」（松島マネージャー）。

ソリューション

これらのインシデントを踏まえ、ソルパックはEDRの情報収集に着手。いくつかのEDRを有力な候補として検証し、最終的にアクロニスの採用を決定しました。

松島マネージャーは「社外に持ち出した業務用PCも管理するため、クラウド型であることは前提条件でした。またアクロニスは管理コンソールも含めたソフトウェアやサポート体制が日本語に対応しており、そのレベルが非常に高かったことが決め手の一つになりました。EDRの多くは機能面に差がなくても英語で提供されているものが大半でしたので、日本語サポートがあることは安心材料になりました」と評価します。

「EDR導入時の懸念事項であったアラート管理の手間がかからないうえ、セキュリティとバックアップがシームレスで連携できる点が安心感につながっています」

株式会社ソルパック
管理本部　本部長
下田 絵理氏

情報システムマネージャー
松島 雅秀氏

またEDRの導入にあたっては管理・運用コストの増加を懸念していたと言います。

「EDRはネットワーク内でサイバー攻撃などが疑われる事象を迅速に捉える一方で、それが本当の脅威に当たるかを人間が都度判定する必要があります。この作業が煩雑になるとかえって必要な対応が後手に回る可能性もあります。こうしたアラート疲労にどう対処するかはEDRを運用するうえでの現実的な課題でしたが、いろいろな製品を見ていくなかでアクロニスのEDRは管理画面が格段に分かりやすく、セキュリティの専門知識を持っていなくても、情報システム部門の人間であれば操作できると思えました」（松島マネージャー）

最大の決め手になったのは、アクロニスがセキュリティとバックアップの両方の機能を兼ね備えていた点です。

「他のEDRツールはセキュリティ機能のみに絞っているものが多く、バックアップとの連携という課題を解決できない可能性がありました。セキュリティとバックアップは車の両輪であり、両者が連携している状況で初めて迅速な業務復旧が可能となります。その点でセキュリティとバックアップを単一コンソールで管理でき、シームレスに連携するAcronis Cyber Protect Cloud Advanced Security + EDRは非常に魅力的でしたね」（下田本部長）

効果と展望

ソルパックは2023年10月にAcronis Cyber Protect Cloud Advanced Security + EDRをはじめとしたアクロニスの各種ツールの導入を開始。約3カ月で社員に貸与するノートPCの50%に当たる約100台へと展開しています。当初はシステムエンジニアなどITリテラシーの高い社員のPCから利用を開始し、実際に使用しながら社内マニュアルを制作したうえで全社展開しています。

下田本部長は「PCへのEDRの導入は、当社の情報システム部門がパッケージしたものを社員がワンクリックするだけで終わります。特別な教育も必要ありません。手間なく始められるという点が、迅速な全社展開につながっています。残るPCについてもできるだけ早めにEDRを導入し、最終的には200台以上に展開する計画です」と話します。

導入前には運用負担の増加を懸念していましたが、アクロニスのEDRは潜在的なインシデントが優先順位付けされるなど効率的な仕組みで、松島マネージャーは「操作の容易さは期待以上です」と評価します。

「例えば社員が構築したExcelのマクロなどがEDRに怪しい挙動として検知される場合があると、情報システム部門ではウイルスか無害なマクロかの判断が付かないため、アラートが出るとその都度、現場の人間に確認を取らなければなりません。アクロニスのEDRであれば管理画面から管理者が容易にウイルスかそうでないかを検証しやすくなっています。セキュリティの専門知識がない社員でも対応しやすく実務面の助けになっています」（松島マネージャー）

今後はAcronis Cyber Protect CloudによるGoogle Workspaceのバックアップなど、より包括的なデータ保護への取り組みを進めていく考えです。各種対策によるビジネス上の効果も見込んでおり、下田本部長は「BPOをはじめ、さまざまなお客様のIT環境をサポートする当社にとってサイバーセキュリティのレベルを高めることは、サービスの魅力を高めることにつながるはずです」と期待を語ります。

Acronis

詳細はwww.acronis.comをご確認ください。

Copyright © 2003-2024 Acronis International GmbH. All rights reserved. AcronisおよびAcronisロゴはAcronis International GmbHの登録商標または商標です。Windowsは米国 Microsoft Corporationの米国およびその他の国における登録商標です。記載されているその他の名称は、各所有者の商標または登録商標である可能性があり、そのような可能性を考慮して扱う必要があります。技術的な変更および図との差異が生じる可能性があり、誤りが含まれている可能性があります。製品仕様は改良のため、予告なく変更になる場合があります。2024-03